

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Yutaka SATA, et al.

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HERewith

FOR: AUTHENTICATION PROCESSING SYSTEM, TERMINAL AUTHENTICATION APPARATUS,  
AUTHENTICATION PROCESSING METHOD AND AUTHENTICATION PROCESSING PROGRAM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:


<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2003-024501	January 31, 2003

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

  
Marvin J. Spivak

Registration No. 24,913

C. Irvin McClelland  
Registration Number 21,124

Customer Number

22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 3 年   1 月 3 1 日  
Date of Application:

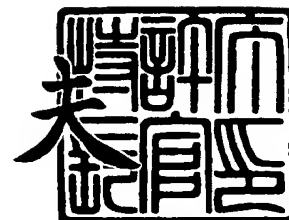
出 願 番 号            特 願 2 0 0 3 - 0 2 4 5 0 1  
Application Number:  
[ST. 10/C]:            [ J P 2 0 0 3 - 0 2 4 5 0 1 ]


出      願      人            株 式 会 社 東 芝  
Applicant(s):

2 0 0 3 年   7 月 1 8 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康



【書類名】 特許願

【整理番号】 13942201

【提出日】 平成15年 1月31日

【あて先】 特許庁長官殿

【国際特許分類】 H04B 7/00

【発明の名称】 認証処理システム、端末認証装置、認証処理方法及び認証処理プログラム

【請求項の数】 18

【発明者】

    【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝  
    研究開発センター内

    【氏名】 佐 田 豊

【発明者】

    【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝  
    研究開発センター内

    【氏名】 杉 川 明 彦

【特許出願人】

    【識別番号】 000003078

    【住所又は居所】 東京都港区芝浦一丁目 1 番 1 号

    【氏名又は名称】 株式会社 東 芝

【代理人】

    【識別番号】 100075812

    【弁理士】

    【氏名又は名称】 吉 武 賢 次

【選任した代理人】

    【識別番号】 100088889

    【弁理士】

    【氏名又は名称】 橋 谷 英 俊

## 【選任した代理人】

【識別番号】 100082991

【弁理士】

【氏名又は名称】 佐 藤 泰 和

## 【選任した代理人】

【識別番号】 100096921

【弁理士】

【氏名又は名称】 吉 元 弘

## 【選任した代理人】

【識別番号】 100103263

【弁理士】

【氏名又は名称】 川 崎 康

## 【手数料の表示】

【予納台帳番号】 087654

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証処理システム、端末認証装置、認証処理方法及び認証処理プログラム

【特許請求の範囲】

【請求項 1】

携帯情報端末と、

前記携帯情報端末との間で、無線にて認証処理を行う端末認証装置と、

前記端末認証装置が前記携帯情報端末との認証に成功した場合に、所定の動作を実行する要認証動作実行装置と、を備えた認証処理システムであって、

前記携帯情報端末は、

第 1 の時間間隔ごとに、前記端末認証装置が存在するか否かを確認するための存在確認信号を送信する存在確認信号送信手段と、

前記存在確認信号に応答して前記端末認証装置から送信された存在通知信号を受信する存在通知信号受信手段と、

前記存在通知信号が受信されると、前記存在通知信号を送信した前記端末認証装置との間で無線リンクを確立する第 1 のリンク接続手段と、

前記無線リンクを介して、前記端末認証装置との間で第 1 の認証を行う第 1 の認証手段と、を有し、

前記端末認証装置は、

第 2 の時間間隔ごとに、前記第 1 の時間間隔と等しいか、又はその間隔よりも長い第 3 の時間間隔の間だけ、前記存在確認信号を受信可能な受信モードに設定される存在確認信号受信手段と、

前記存在確認信号が受信されると、その応答である前記存在通知信号を前記携帯情報端末に送信する存在通知信号送信手段と、

前記存在通知信号が前記携帯情報端末で受信された後に、前記携帯情報端末との間で無線リンクを確立する第 2 のリンク接続手段と、

前記無線リンクを介して、前記携帯情報端末との間で前記第 1 の認証を行う第 2 の認証手段と、

前記第 1 及び第 2 の認証手段による前記第 1 の認証に成功した場合に、前記要

認証動作実行装置に対して制御命令を送信する制御命令送信手段と、を有し、  
前記要認証動作実行装置は、  
前記制御命令を受信する制御命令受信手段と、  
前記制御命令に基づいて前記所定の動作を実行する動作実行手段と、を有する  
ことを特徴とする認証処理システム。

【請求項 2】

携帯情報端末と、  
前記携帯情報端末との間で、無線にて認証処理を行う端末認証装置と、  
前記端末認証装置が前記携帯情報端末との認証に成功した場合に、所定の動作  
を実行する要認証動作実行装置と、を備えた認証処理システムであって、  
前記端末認証装置は、  
第 1 の時間間隔ごとに、前記携帯情報端末が存在するか否かを確認するための  
存在確認信号を送信する存在確認信号送信手段と、  
前記存在確認信号に応答して前記携帯情報端末から送信された存在通知信号を  
受信する存在通知信号受信手段と、  
前記存在通知信号が受信されると、前記存在通知信号を送信した前記携帯情報  
端末との間で無線リンクを確立する第 1 のリンク接続手段と、  
前記無線リンクを介して、前記携帯情報端末との間で第 1 の認証を行う第 1 の  
認証手段と、  
前記第 1 の認証に成功した場合に、前記要認証動作実行装置に対して制御命令  
を送信する制御命令送信手段と、を有し、  
前記携帯情報端末は、  
第 2 の時間間隔ごとに、前記第 1 の時間間隔と等しいか、又はその間隔よりも  
長い第 3 の時間間隔の間だけ、前記存在確認信号を受信可能な受信モードに設定  
される存在確認信号受信手段と、  
前記存在確認信号が受信されると、その応答である前記存在通知信号を前記端  
末認証装置に送信する存在通知信号送信手段と、  
前記存在通知信号が前記端末認証装置で受信された後に、前記端末認証装置と  
の間で無線リンクを確立する第 2 のリンク接続手段と、

前記無線リンクを介して、前記端末認証装置との間で前記第 1 の認証を行う第 2 の認証手段と、を有し、

前記要認証動作実行装置は、

前記制御命令を受信する制御命令受信手段と、

前記制御命令に基づいて前記所定の動作を実行する動作実行手段と、を有することを特徴とする認証処理システム。

#### 【請求項 3】

前記第 1 及び第 2 の時間間隔の和に前記携帯情報端末の平均移動速度を乗じて得られる距離よりも、前記存在確認信号及び前記存在通知信号の電波到達範囲の方が長いことを特徴とする請求項 1 または 2 に記載の認証処理システム。

#### 【請求項 4】

前記携帯情報端末及び前記端末認証装置の少なくとも一方は、前記携帯情報端末と前記端末認証装置との間の距離を検知する距離検知手段を有し、

前記制御命令送信手段は、前記第 1 の認証に成功し、かつ前記携帯情報端末と前記端末認証装置との間の距離が所定値以下になったときに、前記要認証動作実行装置に前記制御命令を送信することを特徴とする請求項 1 及至 3 のいずれかに記載の認証処理システム。

#### 【請求項 5】

前記距離検知手段は、前記携帯情報端末及び前記端末認証装置の間に送受信される電波の電波強度により、距離を検知することを特徴とする請求項 4 に記載の認証処理システム。

#### 【請求項 6】

前記端末認証装置及び前記要認証動作実行装置の少なくとも一方は、前記携帯情報端末またはその所有者が所定距離以内に近づいたことを検知する近接検知手段を備え、

前記動作実行手段は、前記第 1 の認証に成功し、かつ前記制御命令受信手段により前記制御命令が受信され、かつ前記近接検知手段により所定距離以内に近づいたことが検知されたとき、前記所定の動作を実行することを特徴とする請求項 1 及至 5 のいずれかに記載の認証処理システム。

## 【請求項 7】

前記近接検知手段は、前記携帯情報端末の所有者が前記端末認証装置または前記要認証動作実行装置に接触したことを検知する接触検知センサであることを特徴とする請求項 6 に記載の認証処理システム。

## 【請求項 8】

前記携帯情報端末及び前記端末認証装置の少なくとも一方は、前記第 1 の時間間隔よりも前記第 3 の時間間隔の方が長くなるように、前記第 1、第 2 及び第 3 の時間間隔の少なくとも一つを制御するインターバル制御手段を有することを特徴とする請求項 1 及至 7 のいずれかに記載の認証処理システム。

## 【請求項 9】

前記携帯情報端末及び前記端末認証装置の少なくとも一方は、バッテリーの残電気容量を検知するバッテリーモニタ手段を有し、

前記インターバル制御手段は、前記バッテリーモニタ手段で検知されたバッテリーの残電気容量に応じて、前記第 1 及び第 2 の時間間隔が等しくなるように、又は前記第 1 の時間間隔よりも前記第 3 の時間間隔の方が長くなるように、前記第 1、第 2 及び第 3 の時間間隔の少なくとも一つを制御することを特徴とする請求項 8 に記載の認証処理システム。

## 【請求項 10】

前記携帯情報端末及び前記端末認証装置の少なくとも一方は、通信相手を検知できなくなっただけからの経過時間、または前記端末認証装置との間の無線リンクが切断されてからの経過時間を計測する時間計測手段を有し、

前記インターバル制御手段は、前記時間計測手段の計測結果に応じて、前記第 1 及び第 2 の時間間隔が等しくなるように、又は前記第 1 の時間間隔よりも前記第 3 の時間間隔の方が長くなるように、前記第 1、第 2 及び第 3 の時間間隔の少なくとも一つを制御することを特徴とする請求項 8 に記載の認証処理システム。

## 【請求項 11】

前記携帯情報端末は、前記端末認証装置が前記要認証実行装置に前記制御命令を送信した後、前記端末認証装置との間で第 2 の認証を行う第 3 の認証手段を有し、



前記端末認証装置は、前記要認証実行装置に前記制御命令を送信した後、前記携帯情報端末との間で前記第 2 の認証を行う第 4 の認証手段を有することを特徴とする請求項 1 及至 1 0 のいずれかに記載の認証処理システム。

【請求項 1 2】

前記第 1 の認証は、Bluetoothのリンク認証であり、

前記第 2 の認証は、Bluetoothのリンクより上位の認証プロトコルによる認証であることを特徴とする請求項 1 1 に記載の認証処理システム。

【請求項 1 3】

存在確認信号を第 1 の時間間隔ごとに出力する携帯情報端末との間で、無線にて認証処理を行い、前記携帯情報端末との認証に成功した場合に、要認証動作実行装置に対して所定の動作を指示する端末認証装置であって、

第 2 の時間間隔ごとに、前記第 1 の時間間隔と等しいか、又はその間隔よりも長い第 3 の時間間隔の間だけ、前記存在確認信号を受信可能な受信モードに設定される存在確認信号受信手段と、

前記存在確認信号が受信されると、その応答である前記存在通知信号を前記携帯情報端末に送信する存在通知信号送信手段と、

前記存在通知信号が前記携帯情報端末で受信された後に、前記携帯情報端末との間で無線リンクを確立するリンク接続手段と、

前記無線リンクを介して、前記携帯情報端末との間で認証を行う認証手段と、  
前記認証に成功した場合に、前記要認証動作実行装置に対して制御命令を送信する制御命令送信手段と、を有することを特徴とする端末認証装置。

【請求項 1 4】

第 1 の時間間隔ごとに、携帯情報端末が存在するか否かを確認するための存在確認信号を送信する存在確認信号送信手段と、

第 2 の時間間隔ごとに前記第 1 の時間間隔と等しいか、又はその間隔よりも長い第 3 の時間間隔の間だけ前記存在確認信号を受信可能な受信モードに設定される前記携帯情報端末から、前記存在確認信号に応答して送信された存在通知信号を受信する存在通知信号受信手段と、

前記存在通知信号が受信された後に、前記携帯情報端末との間で無線リンクを

確立するリンク接続手段と、

前記無線リンクを介して、前記携帯情報端末との間で認証を行う認証手段と、  
前記認証に成功した場合に、前記要認証動作実行装置に対して制御命令を送信する制御命令送信手段と、を有することを特徴とする端末認証装置。

【請求項 15】

携帯情報端末と、

前記携帯情報端末との間で、無線にて認証処理を行う端末認証装置と、

前記端末認証装置が前記携帯情報端末との認証に成功した場合に、所定の動作を実行する要認証動作実行装置と、を備えた認証処理システムの認証処理方法であって、

前記携帯情報端末は、

第 1 の時間間隔ごとに、前記端末認証装置が存在するか否かを確認するための存在確認信号を送信し、

前記存在確認信号に応答して前記端末認証装置から送信された存在通知信号を受信し、

前記存在通知信号が受信されると、前記存在通知信号を送信した前記端末認証装置との間で無線リンクを確立し、

前記無線リンクを介して、前記端末認証装置との間で認証を行い、

前記端末認証装置は、

第 2 の時間間隔ごとに、前記第 1 の時間間隔と等しいか、又はその間隔よりも長い第 3 の時間間隔の間だけ、前記存在確認信号を受信可能な受信モードに設定され、

前記存在確認信号が受信されると、その応答である前記存在通知信号を前記携帯情報端末に送信し、

前記存在通知信号が前記携帯情報端末で受信された後に、前記携帯情報端末との間で無線リンクを確立し、

前記無線リンクを介して、前記携帯情報端末との間で前記認証を行い、

前記第 1 及び第 2 の認証手段による前記認証に成功した場合に、前記要認証動作実行装置に対して制御命令を送信し、

前記要認証動作実行装置は、  
前記制御命令を受信し、  
前記制御命令に基づいて前記所定の動作を実行することを特徴とする認証処理方法。

【請求項 16】

携帯情報端末と、  
前記携帯情報端末との間で、無線にて認証処理を行う端末認証装置と、  
前記端末認証装置が前記携帯情報端末との認証に成功した場合に、所定の動作を実行する要認証動作実行装置と、を備えた認証処理システムの認証処理方法であって、

前記端末認証装置は、  
第1の時間間隔ごとに、前記携帯情報端末が存在するか否かを確認するための存在確認信号を送信し、  
前記存在確認信号に応答して前記携帯情報端末から送信された存在通知信号を受信し、

前記存在通知信号が受信されると、前記存在通知信号を送信した前記携帯情報端末との間で無線リンクを確立し、

前記無線リンクを介して、前記携帯情報端末との間で第1の認証を行い、  
前記第1の認証に成功した場合に、前記要認証動作実行装置に対して制御命令を送信し、

前記携帯情報端末は、  
第2の時間間隔ごとに、前記第1の時間間隔と等しいか、又はその間隔よりも長い第3の時間間隔の間だけ、前記存在確認信号を受信可能な受信モードに設定され、

前記存在確認信号が受信されると、その応答である前記存在通知信号を前記端末認証装置に送信し、

前記存在通知信号が前記端末認証装置で受信された後に、前記端末認証装置との間で無線リンクを確立し、

前記無線リンクを介して、前記端末認証装置との間で前記第1の認証を行い、

前記要認証動作実行装置は、  
前記制御命令を受信し、  
前記制御命令に基づいて前記所定の動作を実行することを特徴とする認証処理システム。

【請求項 17】

携帯情報端末と、  
前記携帯情報端末との間で、無線にて認証処理を行う端末認証装置と、  
前記端末認証装置が前記携帯情報端末との認証に成功した場合に、所定の動作を実行する要認証動作実行装置と、を備えた認証処理システムのコンピュータ読取可能な認証処理プログラムであって、  
前記携帯情報端末から、第1の時間間隔ごとに、前記端末認証装置が存在するか否かを確認するための存在確認信号を送信し、  
第2の時間間隔ごとに、前記第1の時間間隔と等しいか、又はその間隔よりも長い第3の時間間隔の間だけ、前記端末認証装置を、前記存在確認信号を受信可能な受信モードに設定し、  
前記存在確認信号に応答して前記端末認証装置から送信された存在通知信号を前記携帯情報端末にて受信し、  
前記存在通知信号が受信されると、前記携帯情報端末と前記存在通知信号を送信した前記端末認証装置との間で無線リンクを確立し、  
前記無線リンクを介して、前記携帯情報端末と前記端末認証装置との間で認証を行い、  
前記認証に成功した場合に、前記要認証動作実行装置に対して制御命令を送信し、  
前記制御命令が前記要認証動作実行装置にて受信されると、前記制御命令に基づいて前記所定の動作を実行することを特徴とする認証処理プログラム。

【請求項 18】

携帯情報端末と、  
前記携帯情報端末との間で、無線にて認証処理を行う端末認証装置と、  
前記端末認証装置が前記携帯情報端末との認証に成功した場合に、所定の動作

を実行する要認証動作実行装置と、を備えた認証処理システムのコンピュータ読取可能な認証処理プログラムであって、

前記端末認証装置から、第1の時間間隔ごとに、前記携帯情報端末が存在するか否かを確認するための存在確認信号を送信し、

第2の時間間隔ごとに、前記第1の時間間隔と等しいか、又はその間隔よりも長い第3の時間間隔の間だけ、前記携帯情報端末を、前記存在確認信号を受信可能な受信モードに設定し、

前記存在確認信号に応答して前記携帯情報端末から送信された存在通知信号を前記端末認証装置にて受信し、

前記存在通知信号が受信されると、前記端末認証装置と前記存在通知信号を送信した前記携帯情報端末との間で無線リンクを確立し、

前記無線リンクを介して、前記携帯情報端末と前記端末認証装置の間で認証を行い、

前記認証に成功した場合に、前記端末認証装置から前記要認証動作実行装置に対して制御命令を送信し、

前記制御命令が前記要認証動作実行装置にて受信されると、前記制御命令に基づいて前記所定の動作を実行することを特徴とする認証処理プログラム。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明は、携帯情報端末と端末認証装置との間で認証を行って、認証に成功した場合に所定の動作を許可する認証処理システムに関する。

##### 【0002】

#### 【従来の技術】

物理的な鍵による開錠を必要とせず、ある程度離れた距離より自動車のドア・ロックの開・施錠を行うことができるキーレスシステムが普及してきている。一般的なキーレス・システムは、300MHz以下の微弱電波を用いて、ユーザの持つキーと自動車に設置された無線認証モジュールとの間で認証プロトコルを実行し、認証に成功すると、ドア・ロックの開錠または施錠信号を無線認証モジュールよ

り自動車に送信するものである。微弱電波基地局は、電波法施行規則第六条第一項により規定されるもので、無線局の免許が不要で、300MHz程度であれば約10mの範囲内に電波を発信できるものである。

#### 【0003】

現在最も普及している、キーレスシステムでは、ユーザがドアの開錠（施錠）を行いたいときに、キーに設けられたボタンを押す必要がある。すなわち、ユーザエクスペリエンスは以下になる。

#### 【0004】

(1) 自動車に近づく。(2) パケットや鞆などにしまわれているキーを捜す。(3) キーを取り出す。(4) キーのボタンを押す（開錠）。(5) ユーザがボタン操作を行うと、キーに内蔵される無線モジュールより電波が送信される。

#### 【0005】

一方、自動車に設置される無線認証モジュールは、一定の間隔ごとに、キーからの無線電波の受信を試みている。従って、ユーザがキーのボタン操作を行い、キーより発信される電波が無線認証モジュールで受信されると、その後に認証プロトコルが実行され、ドア・ロックが開錠（施錠）される。キーのボタン操作を行わない場合は、キーからは無線電波が送信されないため、キーに内蔵するバッテリーの寿命（通常の利用で2-5年）を長くすることが可能である。

#### 【0006】

無線電波による開錠の他の問題点、例えば誤開錠を防止するために、開錠後、一定時間で自動的に旋錠されるようにする。乗車のため開錠した後、積み込みに手間取り、時間がかかると自動的に旋錠され、不便を来す。このような問題を解決しようとする発明も知られている（特許文献1を参照）。

#### 【0007】

キーのボタン操作について言えば、キーのバッテリーの消費電力を抑えて寿命を延ばすための操作であるが、この操作はユーザの利便性を低下させている。すなわち、ユーザが鍵の入ったポケット側の手で傘や荷物を持っている場合や、荷物などでユーザの両手がふさがっている場合には、自動車の鍵を開けるには、傘や荷物を持ち帰ったり、荷物をどこかに置く必要がある。

## 【0008】

こういった利便性を改善するために、ボタン操作を不要とするキーレス・システムも提案されている。このシステムでは、基本的には上記と同じ微弱電波を使い、キー側も、一定時間間隔ごとに電波発信モードや受信モードに入り、自動車にキーの無線電波到達範囲に入ると、自動的に認証プロトコルが実行され、ドア・ロックが開錠される。

## 【0009】

上述のキーレス・システムの認証プロトコルに利用される認証（暗号）アルゴリズムとしては、共通鍵方式が一般的に用いられるが、例えばAESなど、最先端の暗号アルゴリズムと十分に長い鍵長を持つ鍵を用いてシステムを構築した場合は、現存する計算機の計算能力では、現実的な時間内に鍵を破り、ドア・ロックを開錠することは不可能であり、通常の物理的鍵と比べて、安全性が高いという特徴もある。

## 【0010】

鍵暗号アルゴリズムの安全性を活かし、自動車エンジンのイグニッションを、暗号アルゴリズムを用いて行う製品も開発されている。イモビライザーと一般的に呼ばれるこのイグニッションキーシステムは、ユーザが自動車のキーを、イグニッションキーホールに挿入し、所定の位置までキーをひねると、キーホールとキーの間に電流信号が流れ、キーに内蔵される認証モジュールとエンジンECUに直結するイモビライザーECUとの間で認証プロトコルが実行されるものである。

## 【0011】

## 【特許文献1】

特開 2001-115707 公報

## 【0012】

## 【発明が解決しようとする課題】

上述したように、自動車のキーは、利便性とセキュリティ性を向上するために、様々な技術を導入している。しかしながら、現在の自動車のキーシステムでは、ユーザは自動車専用のキーを携行しなければ、ドア・ロックの開錠・施錠、エンジンスタートを行うことができない。現在のユーザが日常的に携行するものと

して、携帯電話やPDAに代表される携帯情報端末がある。携帯電話は携帯電話事業者が設置する無線基地局を介して固定電話や他の携帯電話との通話を行ったり、インターネットアクセスを可能とするものであるが、近年、この携帯電話に第二の無線通信装置が搭載される動きが出てきた。この第二の無線通信装置は、原則として極近接～100m程度の電波到達範囲を持ち、携帯電話事業者の提供する基地局を介することなしに、他の端末との通信を可能とするものである。

#### 【0013】

2.4GHz帯のISMバンドとその近傍の周波数を利用し、微弱電力無線機と同様に無線免許が不要であるBluetooth(TM)が注目されている。従来の無線LANの有効な伝送距離範囲が100m以上であるのに対し、Bluetoothは、伝送範囲が狭い分、使用する電力が少ないので、携帯電話などのバッテリーに制限がある情報処理装置に適している。近年、このBluetooth通信手段を搭載した携帯電話やPDA等の携帯型情報処理装置（以下、簡単に携帯情報端末と呼ぶ）が普及し始めている。Bluetoothの詳細は、<http://www.bluetooth.org/>のWebサイトから仕様書が入手できる。

#### 【0014】

携帯情報端末に搭載されるBluetoothやその他の無線通信装置をキーレス・システムとして、自動車などのドア・ロックの開錠や施錠、エンジンイグニッションのスタートなどを行えば、自動車専用のキーを携行しなくて済むようになり、ユーザの利便性は向上する。しかしながら、携帯情報端末に搭載される無線通信装置の主たる目的は、ドア・ロックの開錠・施錠などにあるのではなく、高い転送レートでの情報伝送にあるため、そのキーレス・システムへの応用には、下記のような課題がある。

#### 【0015】

まず、消費電力である。携帯情報端末に搭載される無線通信装置は、上記のとおり、高速なデータ転送を目的として設計されているものであり、現在のキーレス・システムなどに使われている低速、低周波数の無線モジュールと比較すると消費電力が極めて大きい。従って、ユーザが自動車に接近することで、自動的にドア・ロックの開錠を行うようなシステムは、携帯情報端末の消費電力、バッテ



り寿命の視点で、実現が困難である。Bluetoothを用いる場合は、特に特定の端末を発見し、無線リンクを確立する間の消費電力が、通常時の1.5倍以上と大きくなっている。

#### 【0016】

第二の課題は、電波到達範囲である。通常のキーレス・システムでは、ドア・ロックの開錠、施錠を目的として、最適な電波到達範囲、例えば10m程度、を設計、実装することが可能である。ところが、携帯情報端末の無線通信装置は、データ転送を目的として設計されている、また、多くの場合無線規格によって、電波到達範囲がほぼ決まってしまうため、キーレス・システムとして最適な電波到達範囲の設定が難しい。Bluetoothの場合は、携帯情報端末には一般的にClass 3の規格のモジュールが搭載されるが、この電波到達範囲は実効的には20m程度もあり、ユーザが自動車へ接近する意図を持たずに、少し離れたところを通過するだけでも、認証プロトコルが実行され、ドア・ロックが解除されてしまう可能性がある。

#### 【0017】

本発明は、このような点に鑑みてなされたものであり、その目的は、消費電力を削減でき、かつセキュリティ性の高い認証処理システム、端末認証装置、認証処理方法及び認証処理プログラムを提供することにある。

#### 【0018】

##### 【課題を解決するための手段】

上述した課題を解決するために、本発明は、携帯情報端末と、前記携帯情報端末との間で、無線にて認証処理を行う端末認証装置と、前記端末認証装置が前記携帯情報端末との認証に成功した場合に、所定の動作を実行する要認証動作実行装置と、を備えた認証処理システムであって、前記携帯情報端末は、第1の時間間隔ごとに、前記端末認証装置が存在するか否かを確認するための存在確認信号を送信する存在確認信号送信手段と、前記存在確認信号に応答して前記端末認証装置から送信された存在通知信号を受信する存在通知信号受信手段と、前記存在通知信号が受信されると、前記存在通知信号を送信した前記端末認証装置との間で無線リンクを確立する第1のリンク接続手段と、前記無線リンクを介して、前

記端末認証装置との間で第 1 の認証を行う第 1 の認証手段と、を有し、前記端末認証装置は、第 2 の時間間隔ごとに、前記第 1 の時間間隔と等しいか、又はその間隔よりも長い第 3 の時間間隔の間だけ、前記存在確認信号を受信可能な受信モードに設定される存在確認信号受信手段と、前記存在確認信号が受信されると、その応答である前記存在通知信号を前記携帯情報端末に送信する存在通知信号送信手段と、前記存在通知信号が前記携帯情報端末で受信された後に、前記携帯情報端末との間で無線リンクを確立する第 2 のリンク接続手段と、前記無線リンクを介して、前記携帯情報端末との間で前記第 1 の認証を行う第 2 の認証手段と、前記第 1 及び第 2 の認証手段による前記第 1 の認証に成功した場合に、前記要認証動作実行装置に対して制御命令を送信する制御命令送信手段と、を有し、前記要認証動作実行装置は、前記制御命令を受信する制御命令受信手段と、前記制御命令に基づいて前記所定の動作を実行する動作実行手段と、を有する。

#### 【0019】

また、本発明は、携帯情報端末と、前記携帯情報端末との間で、無線にて認証処理を行う端末認証装置と、前記端末認証装置が前記携帯情報端末との認証に成功した場合に、所定の動作を実行する要認証動作実行装置と、を備えた認証処理システムであって、前記端末認証装置は、第 1 の時間間隔ごとに、前記携帯情報端末が存在するか否かを確認するための存在確認信号を送信する存在確認信号送信手段と、前記存在確認信号に応答して前記携帯情報端末から送信された存在通知信号を受信する存在通知信号受信手段と、前記存在通知信号が受信されると、前記存在通知信号を送信した前記携帯情報端末との間で無線リンクを確立する第 1 のリンク接続手段と、前記無線リンクを介して、前記携帯情報端末との間で第 1 の認証を行う第 1 の認証手段と、前記第 1 の認証に成功した場合に、前記要認証動作実行装置に対して制御命令を送信する制御命令送信手段と、を有し、前記携帯情報端末は、第 2 の時間間隔ごとに、前記第 1 の時間間隔と等しいか、又はその間隔よりも長い第 3 の時間間隔の間だけ、前記存在確認信号を受信可能な受信モードに設定される存在確認信号受信手段と、前記存在確認信号が受信されると、その応答である前記存在通知信号を前記端末認証装置に送信する存在通知信号送信手段と、前記存在通知信号が前記端末認証装置で受信された後に、前記端

末認証装置との間で無線リンクを確立する第2のリンク接続手段と、前記無線リンクを介して、前記端末認証装置との間で前記第1の認証を行う第2の認証手段と、を有し、前記要認証動作実行装置は、前記制御命令を受信する制御命令受信手段と、前記制御命令に基づいて前記所定の動作を実行する動作実行手段と、を有する。

### 【0020】

#### 【発明の実施の形態】

以下、本発明に係る認証処理システムの一実施形態について、図面を参照しながら具体的に説明する。

### 【0021】

#### (第1の実施形態)

図1は本発明に係る認証処理システムの第1の実施形態の全体構成を示すブロック図であり、車両用のキーレスエントリを実現するシステムの構成を示している。図1の認証処理システムは、携帯情報端末1と、携帯情報端末1との間で無線にて認証処理を行う端末認証モジュール2と、端末認証モジュール2が携帯情報端末1との認証に成功した場合に車両のエントリ操作を行うエントリ端末3とを備えている。

### 【0022】

携帯情報端末1は、端末認証モジュール2が存在するか否かを確認するための存在確認信号を送信する存在確認信号送信部11と、存在確認信号に応答して端末認証モジュール2から送信された存在通知信号を受信する存在通知信号受信部12と、存在通知信号を送信した端末認証モジュール2との間で無線リンクを確立するリンク接続部13と、無線リンクを介して端末認証モジュール2との間で第1の認証を行う第1の認証部14とを有する。

### 【0023】

また、端末認証モジュール2は、存在確認信号を受信する存在確認信号受信部21と、存在確認信号に対する応答である存在通知信号を送信する存在通知信号送信部22と、存在通知信号が携帯情報端末1で受信された後に携帯情報端末1との間で無線リンクを確立するリンク接続部23と、無線リンクを介して携帯情

報端末 1 との間で第 1 の認証を行う第 2 の認証部 24 と、第 1 の認証に成功した場合にエントリ端末 3 に対して制御命令を送信する制御命令送信部 25 とを有する。

#### 【0024】

エントリ端末 3 は、制御命令を受信する制御命令受信部 31 と、制御命令に基づいて所定のエントリ操作を実行するエントリ部 32 とを有する。ここで、所定のエントリ操作とは、例えば、ドアロックの解除や、イグニッションの開始などの操作である。

#### 【0025】

図 2 は、携帯情報端末 1、端末認証モジュール 2 及びエントリ端末 3 の動作タイミング図である。図 2 に示すように、携帯情報端末 1 は、第 1 の時間間隔ごとに存在確認信号を送信する。端末認証モジュール 2 は、第 2 の時間間隔ごとに、第 1 の時間間隔と等しいか、又はその間隔よりも長い第 3 の時間間隔の間だけ、存在確認信号を受信する受信モードになる。端末認証モジュール 2 は、受信モードに設定されたときだけ存在確認信号を受信する。

#### 【0026】

図 2 の破線で示す期間は、端末認証モジュール 2 が携帯情報端末 1 の電波到達範囲内に存在しないことを示している。したがって、この期間内に携帯情報端末 1 が存在確認信号を送信しても、端末認証モジュール 2 は存在通知信号を送信しない。このため、携帯情報端末 1 は繰り返し存在確認信号を送信することになる。

#### 【0027】

ただし、第 3 の時間間隔を第 1 の時間間隔と等しいか、又は第 1 の時間間隔よりも長く設定しているため、携帯情報端末 1 と端末認証モジュール 2 が互いに電波到達範囲内に位置すれば、端末認証モジュール 2 は携帯情報端末 1 からの存在確認信号を所定時間内に必ず受信することができる。

#### 【0028】

携帯情報端末 1 と端末認証モジュール 2 は、例えば Bluetooth で電波の送受信を行う。Bluetooth では、存在確認信号の送信は Page モードに相当し、存在確認

信号の受信はPage scanモードに相当するが、時間的に連続してPageモードまたはPage scanモードに入ると、Bluetoothモジュールの消費電力が大きくなる。これに対して、本実施形態では、第1の時間間隔ごとに存在確認信号を送信し、また端末認証モジュール2は第2の時間間隔ごとに第3の時間間隔だけ受信モードに設定されるため、時間的に連続して存在確認信号を送受信するよりも、消費電力を削減できる。

#### 【0029】

端末認証モジュール2の存在確認信号受信部21は、携帯情報端末1からの存在確認信号を受信すると、直ちに携帯情報端末1に存在通知信号を送信する。携帯情報端末1は、端末認証モジュール2からの存在通知信号を受信すると、リンク接続部13を用いて、端末認証モジュール2に対してリンク接続要求を出力する。これにより、端末認証モジュール2のリンク接続部23との間で無線リンク接続トランザクションが実行され、無線リンクが確立される。

#### 【0030】

次に、無線リンク上で、携帯情報端末1の第1の認証部14と端末認証モジュール2の第2の認証部24との間で双方向認証（第1の認証）のトランザクションが実行され、双方向認証に成功すると、端末認証モジュール2の制御命令送信部25に第1の認証が正常に終了したことが通知される。制御命令送信部25は、エントリ端末3の制御命令受信部31に対して制御命令を送信し、この制御命令を受信したエントリ端末3は、所定のエントリ操作を行う。例えば、エントリ端末3が自動車で、エントリ部32がドアロック制御部の場合には、制御命令を受信した後に、ドアロックを解除する。

#### 【0031】

図3は端末認証モジュール2の電波到達範囲を示す代表半径と携帯情報端末1の代表移動速度との関係を示す図である。図2のような第1～第3の時間間隔が設定されている場合、携帯情報端末1が電波到達範囲内に入ってから、携帯情報端末1が端末認証モジュール2から存在通知信号を受信するまでの統計的平均時間と最大時間はそれぞれ（1）式及び（2）式で表される。

#### 【0032】

$$\text{平均受信時間} = (\text{第 1 の時間間隔} + \text{第 2 の時間間隔}) / 2 \quad \cdots (1)$$

$$\text{最大時間} = (\text{第 1 の時間間隔} + \text{第 2 の時間間隔}) \quad \cdots (2)$$

したがって、携帯情報端末 1 が図示しないエントリ端末 3 にエントリするために、端末認証モジュール 2 に向かって代表速度で接近する場合、(2) 式に示す最大時間に代表速度を乗じた値よりも、電波到達範囲の代表半径が大きければ、携帯情報端末 1 はエントリ端末 3 に近接する前に端末認証モジュール 2 の存在を検知し、所定の認証プロトコルを実行して、エントリ端末 3 にエントリ操作を行わせることが可能となる。

#### 【0033】

このように、第 1 の実施形態では、携帯情報端末 1 が第 1 の時間間隔ごとに存在確認信号を送信し、端末認証モジュール 2 が第 2 の時間間隔ごとに第 3 の時間間隔の間だけ存在確認信号を受信する受信モードに設定されるため、携帯情報端末 1 と端末認証モジュール 2 の双方とも消費電力を削減できる。また、携帯情報端末 1 と端末認証モジュール 2 との間の認証に成功した場合に限り、エントリ端末 3 のエントリ操作を許可するため、セキュリティ性能を向上できる。さらに、第 1 の時間間隔と第 3 の時間間隔を同じ長さか、第 1 の時間間隔よりも第 3 の時間間隔を長く設定するため、端末認証モジュール 2 は所定時間内に必ず存在確認信号を受信でき、携帯情報端末 1 と端末認証モジュール 2 との間でのリンク確立に要する時間を短縮化できる。

#### 【0034】

##### (第 2 の実施形態)

第 1 の実施形態では、携帯情報端末 1 が存在確認信号を送信し、端末認証モジュール 2 が存在確認信号の応答信号である存在通知信号を送信する例を説明したが、以下に説明する第 2 の実施形態は、端末認証モジュール 2 が存在確認信号を送信し、携帯情報端末 1 が存在通知信号を送信するものである。

#### 【0035】

図 4 は本発明に係る認証処理システムの第 2 の実施形態の全体構成を示すブロック図である。図 4 では、図 1 と共通する構成部分には同一符号を付しており、以下では相違点を中心に説明する。

## 【0036】

図4の携帯情報端末1は、存在確認信号受信部15と、存在通知信号送信部16と、リンク接続部13と、第1の認証部14とを有する。また、端末認証モジュール2は、存在確認信号送信部26と、存在通知信号受信部27と、リンク接続部13と、第2の認証部24とを有する。

## 【0037】

端末認証モジュール2の存在確認信号送信部26は、携帯情報端末1に対して、第1の時間間隔ごとに存在確認信号を送信する。携帯情報端末1は、第2の時間間隔ごとに第3の時間間隔の間だけ存在確認信号を受信可能な受信モードに設定される。この受信モード期間内に、携帯情報端末1内の存在確認信号受信部15にて存在確認信号が受信されると、存在通知信号送信部16は存在通知信号を送信する。この存在通知信号を端末認証モジュール2が内の存在通知信号受信部27が受信すると、携帯情報端末1と端末認証モジュール2との間で無線リンクを接続する処理が行われる。

## 【0038】

このように、第2の実施形態においても、携帯情報端末1と端末認証モジュール2が所定時間ごとに存在確認信号の受け渡しを行うため、携帯情報端末1と端末認証モジュール2の双方とも消費電力を削減できる。

## 【0039】

(第3の実施形態)

第3の実施形態は、携帯情報端末1と端末認証モジュール2との距離を検出するものである。

## 【0040】

図5は本発明に係る認証処理システムの第3の実施形態の全体構成を示すブロック図、図6は図5の認証処理システムのシーケンス図である。図5の認証処理システムの端末認証モジュール2は、図1の構成に加えて、さらに無線電波強度計測部28を有する。

## 【0041】

無線電波強度計測部28は、携帯情報端末1から送信されたリファレンス信号

の電波強度を測定し、その測定値を予め設定したしきい値と比較する（図6の時刻  $t_1$ 、 $t_2$ ）。電波強度の測定値がしきい値よりも大きければ、携帯情報端末1が端末認証モジュール2に近接したと判断し、無線電波強度計測部28は、制御命令送信部25にその旨を伝達する。制御命令送信部25は、第1の認証に成功し、かつ携帯情報端末1が端末認証モジュール2に近接したと判断された場合に、エントリ端末3の制御命令受信部31に制御命令を送る。

#### 【0042】

以上のシステム構成とシーケンスにより、携帯情報端末1と端末認証モジュール2の電波到達範囲がエントリ端末3の操作に最適な距離よりも大きい場合には、この最適な距離内に携帯情報端末1が位置する場合のみ、エントリ端末3のエントリ操作を許可するように制御することができる。

#### 【0043】

なお、無線電波強度測定部28を、端末認証モジュール2の内部ではなく、携帯情報端末1の内部に設けてもよい。また、エントリ端末3の内部に、携帯情報端末1との距離を測定する距離測定部を設けてもよい。この距離測定部は、無線電波強度測定部28と同様の電波強度により距離を測定するものであってもよいし、送信電波が返ってくるまでの遅延時間により距離を測定したり、赤外線等により距離を測定してもよいし、あるいは接触検知センサで携帯情報端末1のユーザが接触したことを検知してもよい。例えば、車両の場合は、より具体的には、ドアノブに設けられたタッチセンサやエントリ端末3に設けられた赤外線センサなどである。

#### 【0044】

エントリ端末3の内部に距離測定部を設けた場合は、携帯情報端末1と端末認証モジュール2との双方向認証が正常に終了した後、端末認証モジュール2がエントリ端末3に制御命令を通知し、エントリ端末3が制御命令受信部31で制御命令を受信した後に、距離測定部で携帯情報端末1が近接したことを検知し、所定のエントリ操作を行う。

#### 【0045】

このように、第3の実施形態では、携帯情報端末1が近接したか否かを検知し



、携帯情報端末 1 が所定距離以内に近接した場合のみ、エントリ端末 3 のエントリ操作を許可するようにしたため、図 3 の電波到達範囲が広くて、携帯情報端末 1 が離れているのに認証に成功した場合であっても、携帯情報端末 1 が近づくまではエントリ端末 3 のエントリ操作を禁止でき、セキュリティ性能がより向上する。

#### 【0046】

##### (第 4 の実施形態)

第 4 の実施形態は、バッテリーの残電気容量に応じて、上述した第 1 ～ 第 3 の時間間隔を制御するものである。

#### 【0047】

図 7 は本発明に係る認証処理システムの第 4 の実施形態のブロック図である。図の携帯情報端末 1 は、図 5 の構成に加えて、携帯情報端末 1 のメイン電源であるバッテリー 17 と、バッテリー 17 の残電気容量をモニタするバッテリーモニタ部 18 と、存在確認信号を送信する時間間隔である第 1 の時間間隔を調整するインターバル制御部 19 とを有する。

#### 【0048】

また、図 7 の端末認証モジュール 2 は、図 5 の構成に加えて、端末認証モジュール 2 のメイン電源であるバッテリー 29 と、バッテリー 29 の残電気容量をモニタするバッテリーモニタ部 41 と、インターバル制御部 42 とを有する。インターバル制御部 42 は、存在確認信号を受信可能な受信モードに設定する時間間隔である第 2 の時間間隔と、受信モードの期間である第 3 の時間間隔との少なくとも一方の時間長を調整する。

#### 【0049】

図 8 は携帯情報端末 1 のインターバル制御部 19 の処理手順を示すフローチャートである。まず、端末認証モジュール 2 との無線リンクが接続中であるか否かを判定し（ステップ S1）、接続中であればステップ S1 に留まり、接続中でなければバッテリーモニタ部 18 にてバッテリー 17 の残電気容量を確認する（ステップ S2）。

#### 【0050】

次に、バッテリー 17 の残電気容量が所定のしきい値より多いか否かを判定し（ステップ S3）、多い場合には、第 1 の時間間隔が所定値 T1 であるか否かを判定する（ステップ S4）。所定値 T1 であれば、第 1 の時間間隔を変更せずにステップ S1 に戻り、所定値 T1 でなければ、第 1 の時間間隔を所定値 T1 に設定して（ステップ S5）、ステップ S1 に戻る。

#### 【0051】

一方、ステップ S3 で、バッテリー 17 の残電気容量が所定のしきい値以下と判定された場合には、第 1 の時間間隔が所定値 T2 であるか否かを判定し（ステップ S6）、所定値 T2 であれば、第 1 の時間間隔を変更せずにステップ S1 に戻り、所定値 T2 でなければ、第 1 の時間間隔を所定値 T2 に設定して（ステップ S7）、ステップ S1 に戻る。

#### 【0052】

より具体的には、携帯情報端末 1 のインターバル制御部 19 は、バッテリー 17 の残電気容量が少なくなるほど、第 1 の時間間隔を長くして、携帯情報端末 1 の電力消費量を減らす。一方、バッテリー 17 の残電気容量に余裕がある場合には、第 1 の時間間隔を短くし、端末認証モジュール 2 との間の無線リンク確立までの時間短縮を図れる。

#### 【0053】

端末認証モジュール 2 のインターバル制御部 42 も、図 6 と同様の処理を行う。なお、携帯情報端末 1 と端末認証モジュール 2 のいずれか一方のみに、インターバル制御部を設けてもよい。

#### 【0054】

ところで、携帯情報端末 1 と端末認証モジュール 2 が、それぞれ無関係に第 1 ～第 3 の時間間隔を調整すると、存在確認信号の送信間隔である第 1 の時間間隔が、端末認証モジュール 2 の受信モード継続期間である第 3 の時間間隔よりも長くなる場合がありうる。この場合、端末認証モジュール 2 は、携帯情報端末 1 からの存在確認信号を受信できなくなってしまう。

#### 【0055】

このため、携帯情報端末 1 のインターバル制御部 19 は、第 1 の時間間隔が第

3の時間間隔か、又は等しくなるような範囲内で第1の時間間隔を調整する必要がある。

#### 【0056】

このように、第3の実施形態では、携帯情報端末1や端末認証モジュール2のインターバル制御部19、42にて、バッテリー17、29の残電気容量に応じて第1～第3の時間間隔の少なくとも一つを制御するようにしたため、バッテリー17、29の残電気容量が少なくなった場合の携帯情報端末1や端末認証モジュール2の電力消費量を削減できる。

#### 【0057】

なお、図7に点線で示すように、携帯情報端末1と端末認証モジュール2の少なくとも一方にタイマ43、44を設け、このタイマ43、44で例えば無線リンクを切断してからの経過時間を計測し、その計測時間により第1～第3の時間間隔を設定してもよい。

#### 【0058】

(第5の実施形態)

第5の実施形態は、二重に認証を行うものである。

#### 【0059】

図9は本発明に係る認証処理システムの第5の実施形態の全体構成を示すブロック図である。図9の携帯情報端末1は、図1の構成に加えて、端末認証モジュール2がエントリ端末3に制御命令を送信した後、端末認証モジュール2との間で第2の認証を行う第3の認証部44を有する。

#### 【0060】

図9の端末認証モジュール2は、図1の構成に加えて、エントリ端末3からの認証要求を受信する認証要求受信部45と、エントリ端末3に制御命令を送信した後に携帯情報端末1との間で第2の認証を行う第4の認証部46とを有する。また、図9のエントリ端末3は、図1の構成に加えて、携帯情報端末1のユーザがエントリ端末3に接触したことを検知する接触式近接検知センサ33と、端末認証モジュール2に対して認証要求を行う認証要求部34とを有する。

#### 【0061】

図10は第5の実施形態の認証処理システムの処理手順を示すフローチャートである。まず、端末認証モジュール2は、第2の時間間隔ごとに、第3の時間間隔の間だけ受信モードにして、携帯情報端末1からの存在確認信号が受信されたか否かを判定する（ステップS21）。

#### 【0062】

存在確認信号が受信されると、携帯情報端末1に存在通知信号を送信した後に、携帯情報端末1との間で無線リンクを確立し（ステップS22）、第2の認証部24は、例えばBluetoothのリンク認証を実行する（ステップS23）。リンク認証により双方向認証（第1の認証）が確認されると、制御命令送信部25は、第1の認証に対応するエントリ端末3の第1のエントリ操作を実行するための制御命令をエントリ端末3に送信する（ステップS24）。

#### 【0063】

エントリ端末3は、端末認証モジュール2からの制御命令を受信すると（ステップS25）、第1のエントリ操作を実行し（ステップS26）、同時に接触式近接検知センサ33を作動させる（ステップS27）。ここで、第1のエントリ操作とは、例えば、車両のドアロックを解除する操作であり、この時点では、ドアロックは解除しても、イグニッションのスタートは許可されない。

#### 【0064】

接触式近接検知センサ33が携帯情報端末1の近接を検知すると（ステップS28）、エントリ端末3の認証要求部34は端末認証モジュール2に第2の認証要求を行う（ステップS29）。

#### 【0065】

この認証要求を端末認証モジュール2の認証要求受信部が受信すると、第4の認証部46は、Bluetoothリンクの上位でアプリケーション認証（第2の認証）を実行する（ステップS30）。このアプリケーション認証は、第2の認証部24が行う認証よりも、より安全性の高い認証手続である。

#### 【0066】

携帯情報端末1との間で再度の認証に成功すると（ステップS31）、制御命令送信部25は、第2の認証に対応する第2のエントリ操作を実行するための制

御命令をエントリ端末3に送信する（ステップS32）。

#### 【0067】

この制御命令をエントリ端末3の制御命令受信部31が受信すると（ステップS33）、エントリ部32は第2のエントリ処理を実行する（ステップS34）。ここで、第2のエントリ操作とは、例えば、イグニッションのスタートを許可する操作であり、ステップS34の処理を行うことで、携帯情報端末1のユーザは車両のエンジンをかけることができる。

#### 【0068】

このように、第4の実施形態では、複数のエントリ操作のそれぞれに別個の認証を行うため、セキュリティ性能をより向上できる。

#### 【0069】

上述した図9の認証処理システムでは、エントリ端末3内に接触式近接検知センサ33を設けたが、端末認証モジュール2内に接触式近接検知センサを設けてもよい。この場合の全体構成は図11のようなブロック図で表される。図示のように、端末認証モジュール2に接触式近接検知センサ47が設けられる。この接触式近接検知センサ47で、携帯情報端末1の接触が検知されると、検知されたことが第4の認証部46に送られて、第4の認証部46は第2の認証を行う。

#### 【0070】

図11の場合、エントリ端末3から端末認証モジュール2に認証要求を送る必要がないため、エントリ端末3の構成を簡略化できる。

#### 【0071】

なお、第4の実施形態において、3つ以上のエントリ操作を設けて、それぞれに別個の認証を行ってもよい。

#### 【0072】

上述した実施形態で説明した認証処理システムは、ハードウェアで構成してもよいし、ソフトウェアで構成してもよい。ソフトウェアで構成する場合には、認証処理システムの機能を実現するプログラムをフロッピーディスクやCD-ROM等の記録媒体に収納し、コンピュータに読み込ませて実行させてもよい。記録媒体は、磁気ディスクや光ディスク等の携帯可能なものに限定されず、ハードデ

ISK装置やメモリなどの固定型の記録媒体でもよい。

### 【0073】

また、認証処理システムの機能を実現するプログラムを、インターネット等の通信回線（無線通信も含む）を介して頒布してもよい。さらに、同プログラムを暗号化したり、変調をかけたり、圧縮した状態で、インターネット等の有線回線や無線回線を介して、あるいは記録媒体に収納して頒布してもよい。

### 【0074】

#### 【発明の効果】

以上詳細に説明したように、本発明によれば、携帯情報端末が存在確認信号を第1の時間間隔で出力し、端末認証装置は第2の時間間隔ごとに第3の時間間隔の間だけ存在確認信号の受信を受け付けるため、携帯情報端末と端末認証装置がともに消費電力を削減できる。また、携帯情報端末と端末認証装置との間での認証に成功した場合に限り、要認証動作実行装置が所定の動作を実行するようにしたため、セキュリティ性能を向上できる。さらに、第1の時間間隔を第3の時間間隔と等しくか、又は第1の時間間隔よりも第3の時間間隔を長くしたため、端末認証装置は必ず携帯情報端末からの存在確認信号を受信できる。

#### 【図面の簡単な説明】

#### 【図1】

本発明に係る認証処理システムの第1の実施形態の全体構成を示すブロック図。

#### 【図2】

携帯情報端末1、端末認証モジュール2及びエントリ端末3の動作タイミング図。

#### 【図3】

端末認証モジュール2の電波到達範囲を示す代表半径と携帯情報端末1の代表移動速度との関係を示す図。

#### 【図4】

本発明に係る認証処理システムの第2の実施形態の全体構成を示すブロック図。

## 【図 5】

本発明に係る認証処理システムの第 3 の実施形態の全体構成を示すブロック図

。

## 【図 6】

図 5 の認証処理システムのシーケンス図。

## 【図 7】

本発明に係る認証処理システムの第 4 の実施形態のブロック図。

## 【図 8】

携帯情報端末 1 のインターバル制御部 19 の処理手順を示すフローチャート。

## 【図 9】

本発明に係る認証処理システムの第 5 の実施形態の全体構成を示すブロック図

。

## 【図 10】

第 5 の実施形態の認証処理システムの処理手順を示すフローチャート。

## 【図 11】

端末認証モジュール内に接触式近接検知センサを設けた場合の全体構成を示すブロック図。

## 【符号の説明】

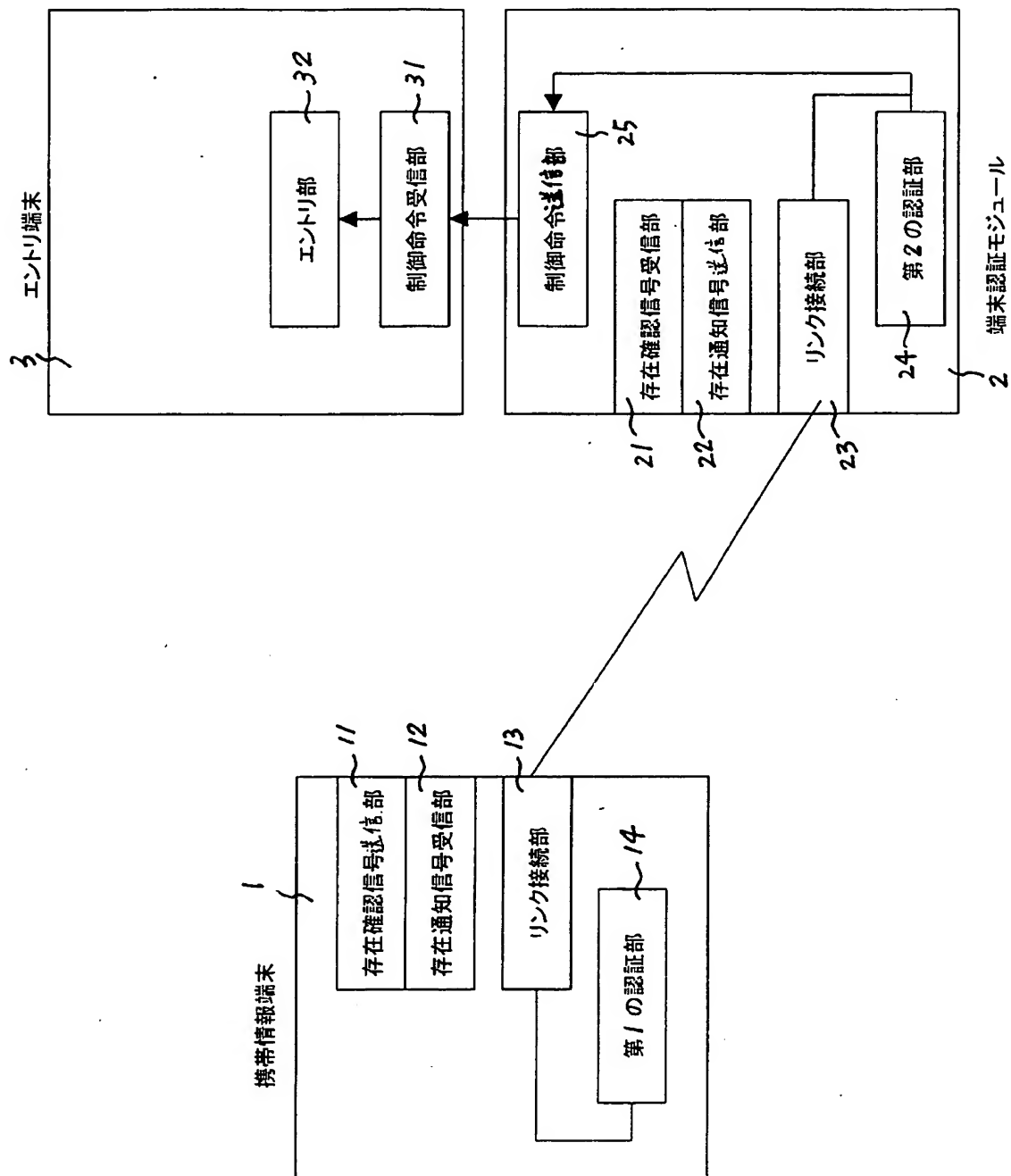
- 1 携帯情報端末
- 2 端末認証モジュール
- 3 エントリ端末
  - 11 存在確認信号送信部
  - 12 存在通知信号受信部
  - 13 リンク接続部
  - 14 第 1 の認証部
  - 15 存在確認信号受信部
  - 16 存在通知信号送信部
- 21 存在確認信号受信部
- 22 存在通知信号送信部

- 2 3 リンク接続部
- 2 4 第 2 の認証部
- 2 5 制御命令送信部
- 2 6 存在確認信号送信部
- 2 7 存在通知信号受信部
- 2 8 無線電波強度計測部
- 3 1 制御命令受信部
- 3 2 エントリ部

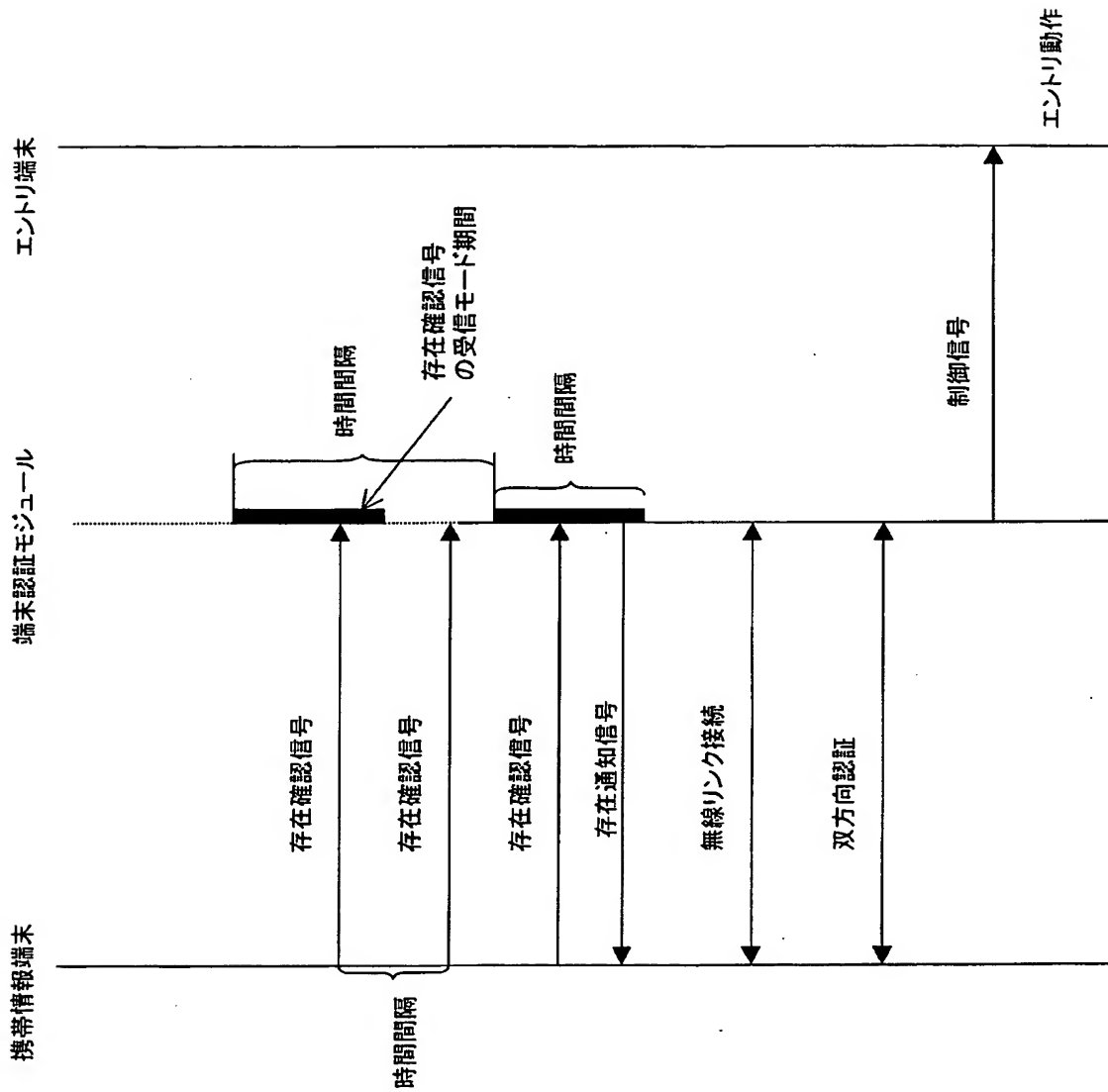


【書類名】 図面

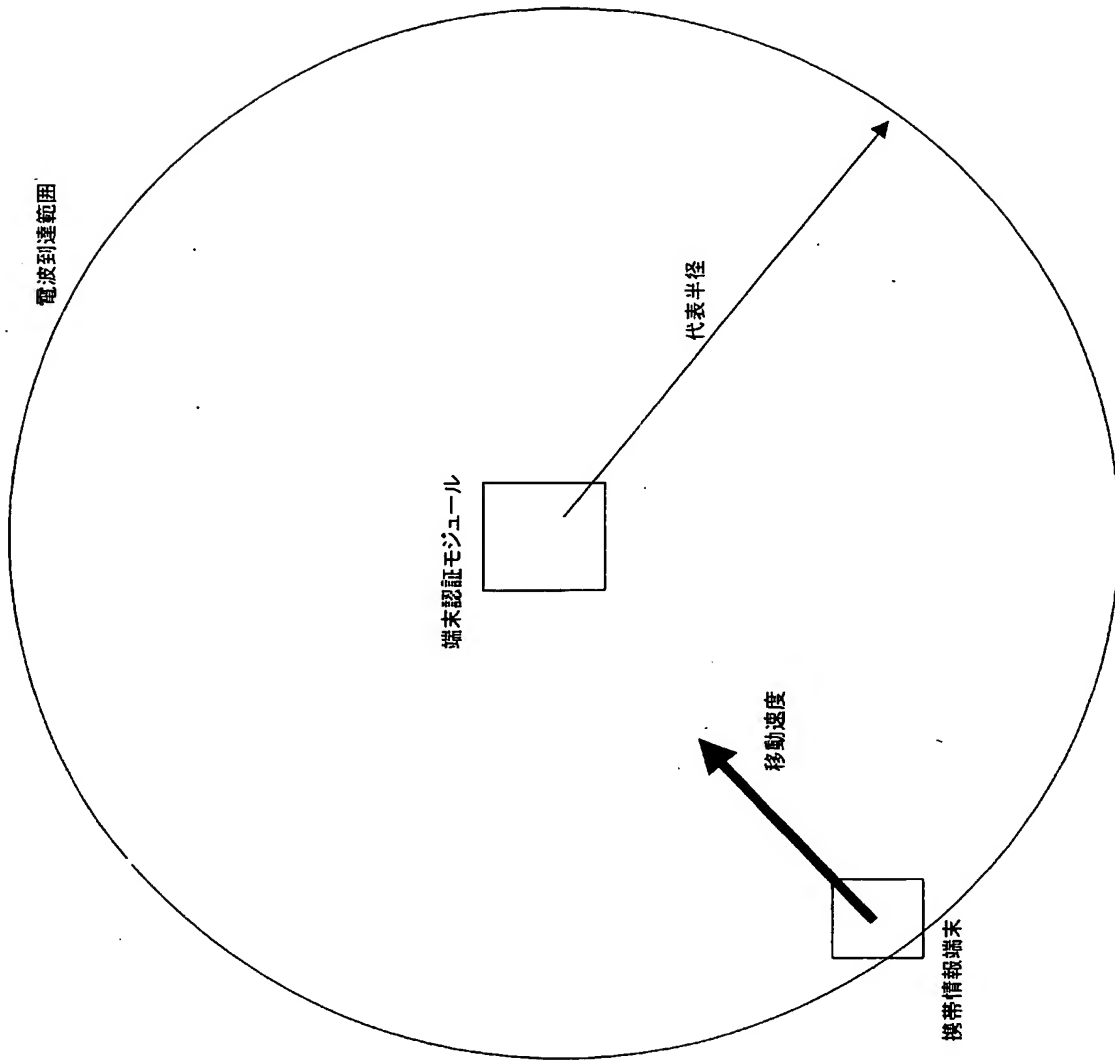
【図 1】



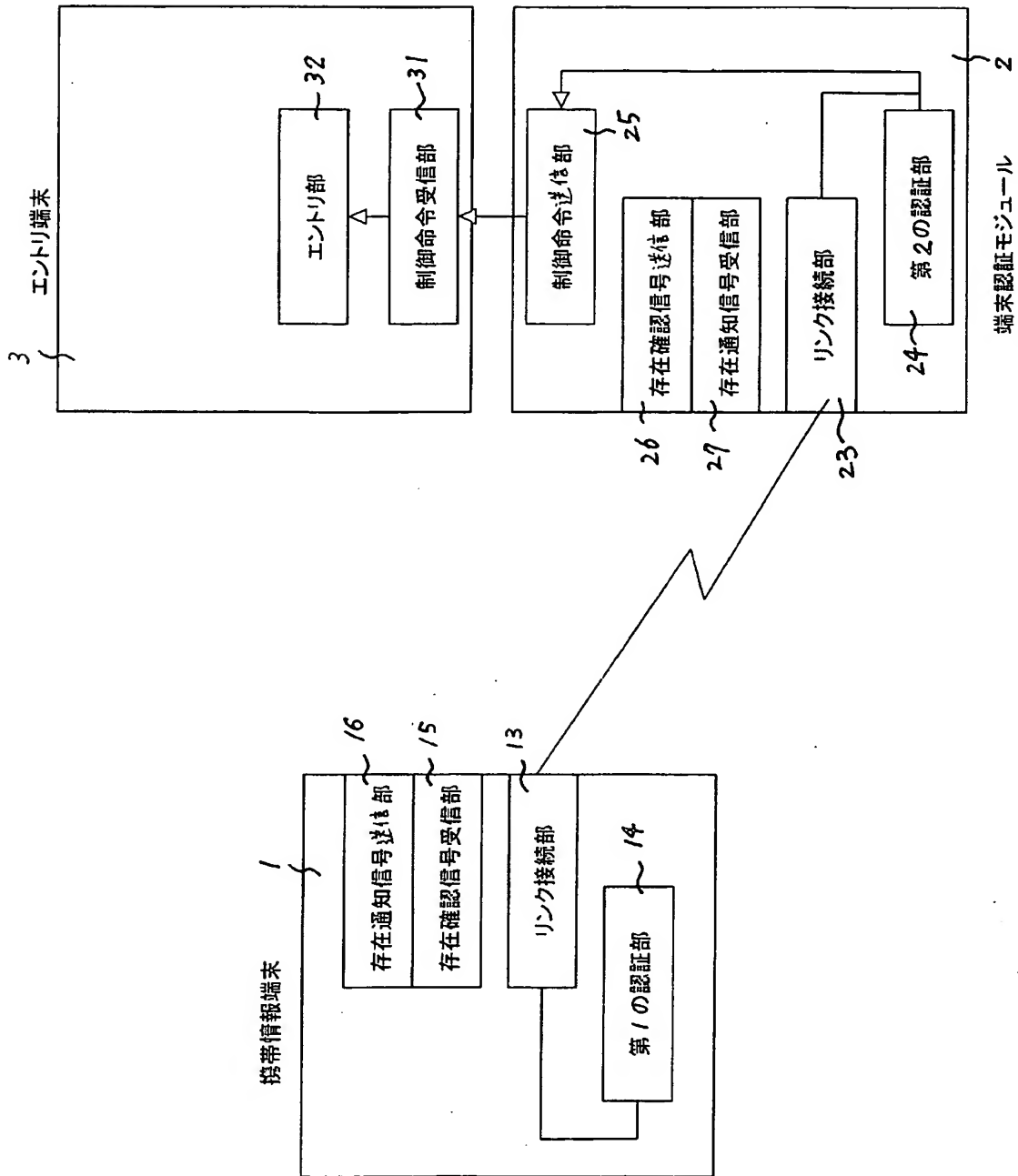
【図 2】



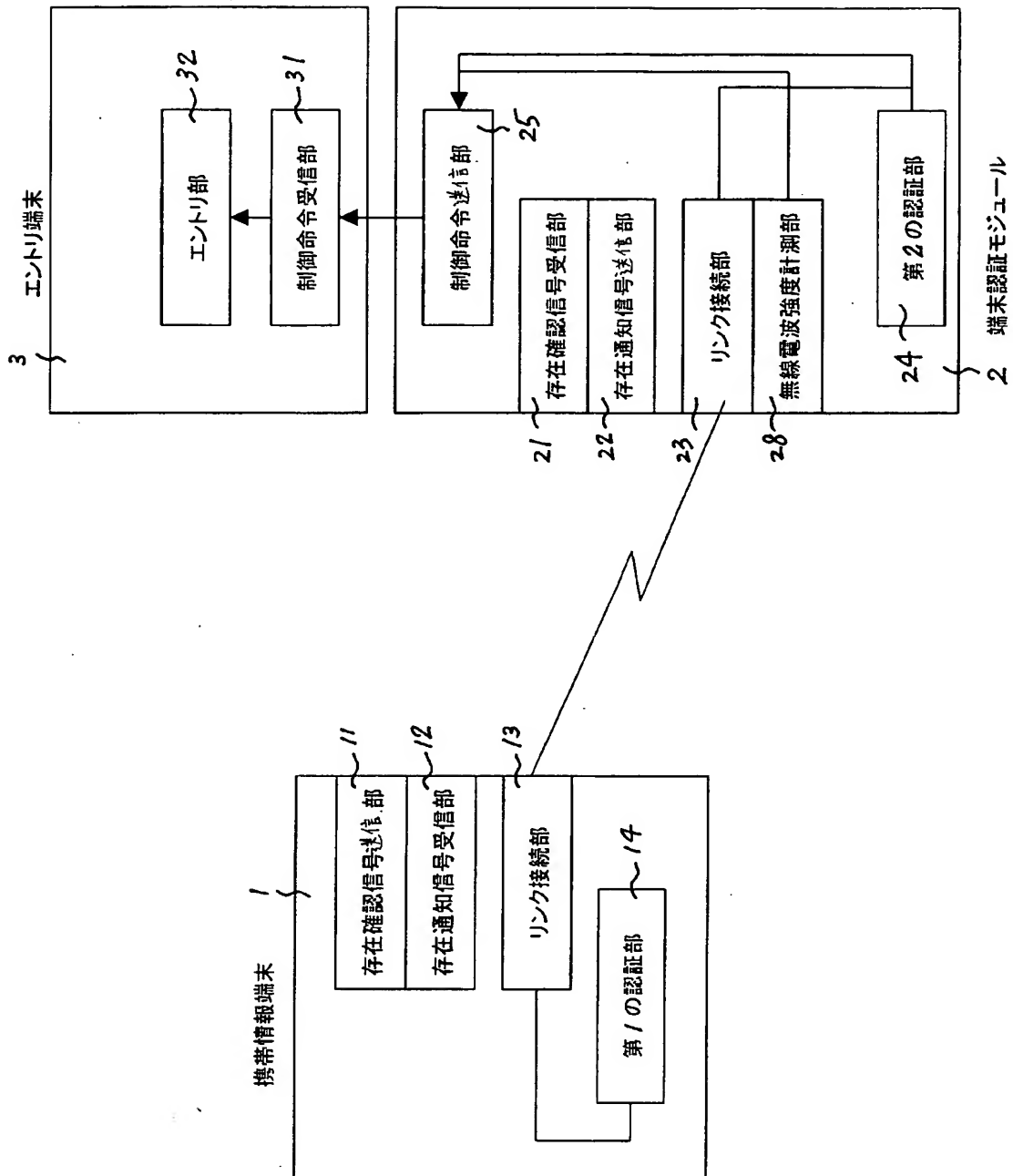
【図 3】



【図 4】

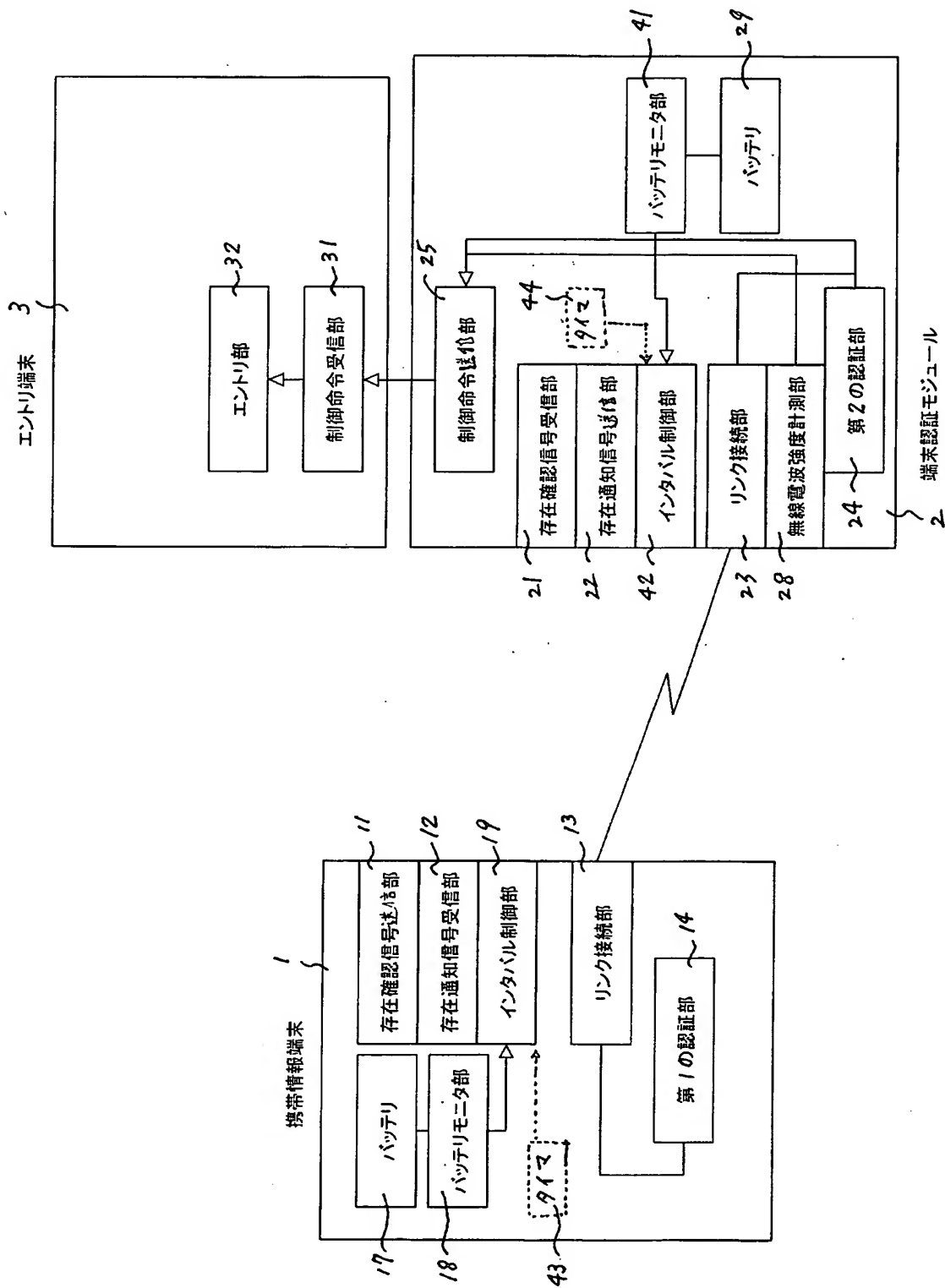


【図 5】

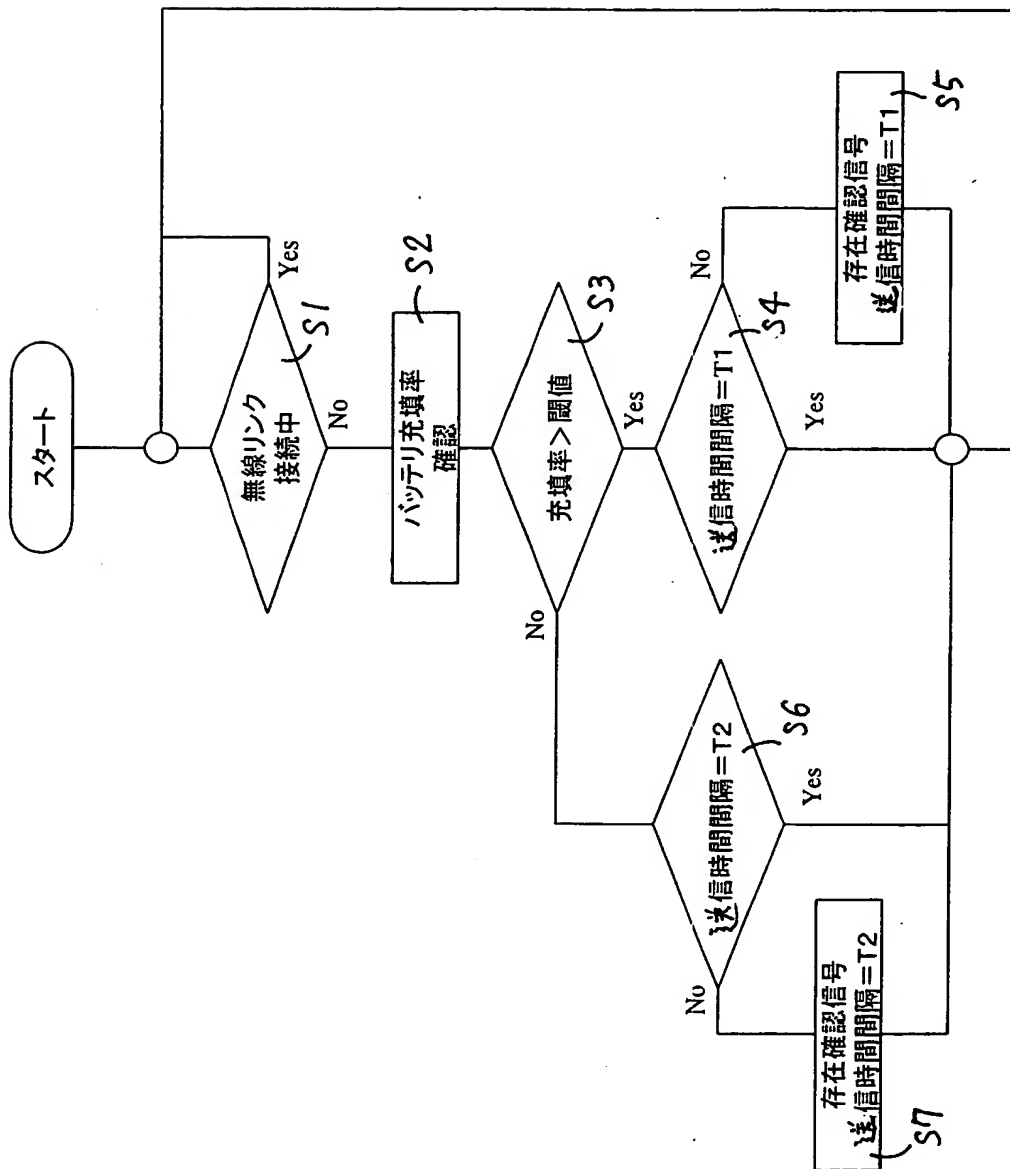




【图 7】

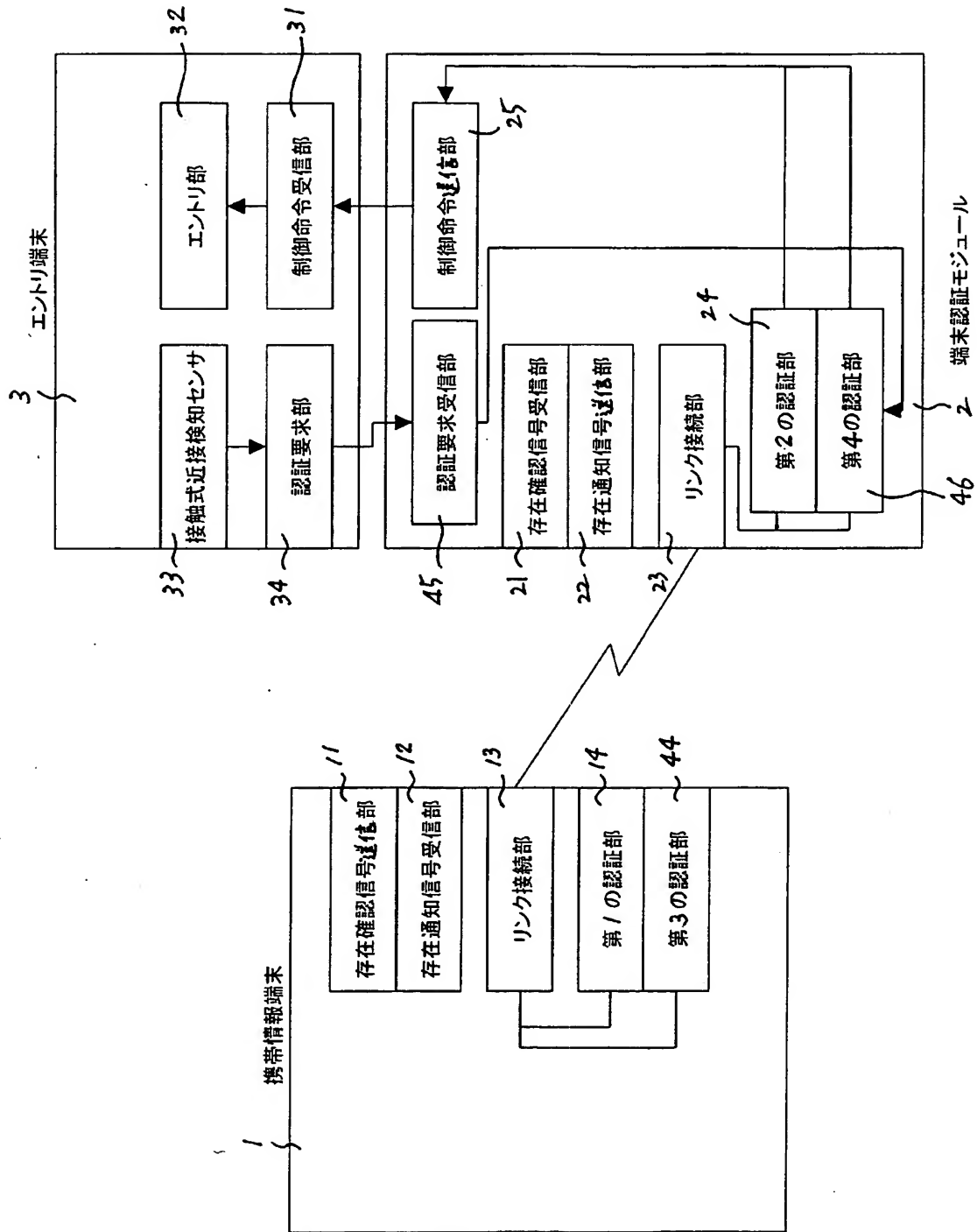


【図 8】

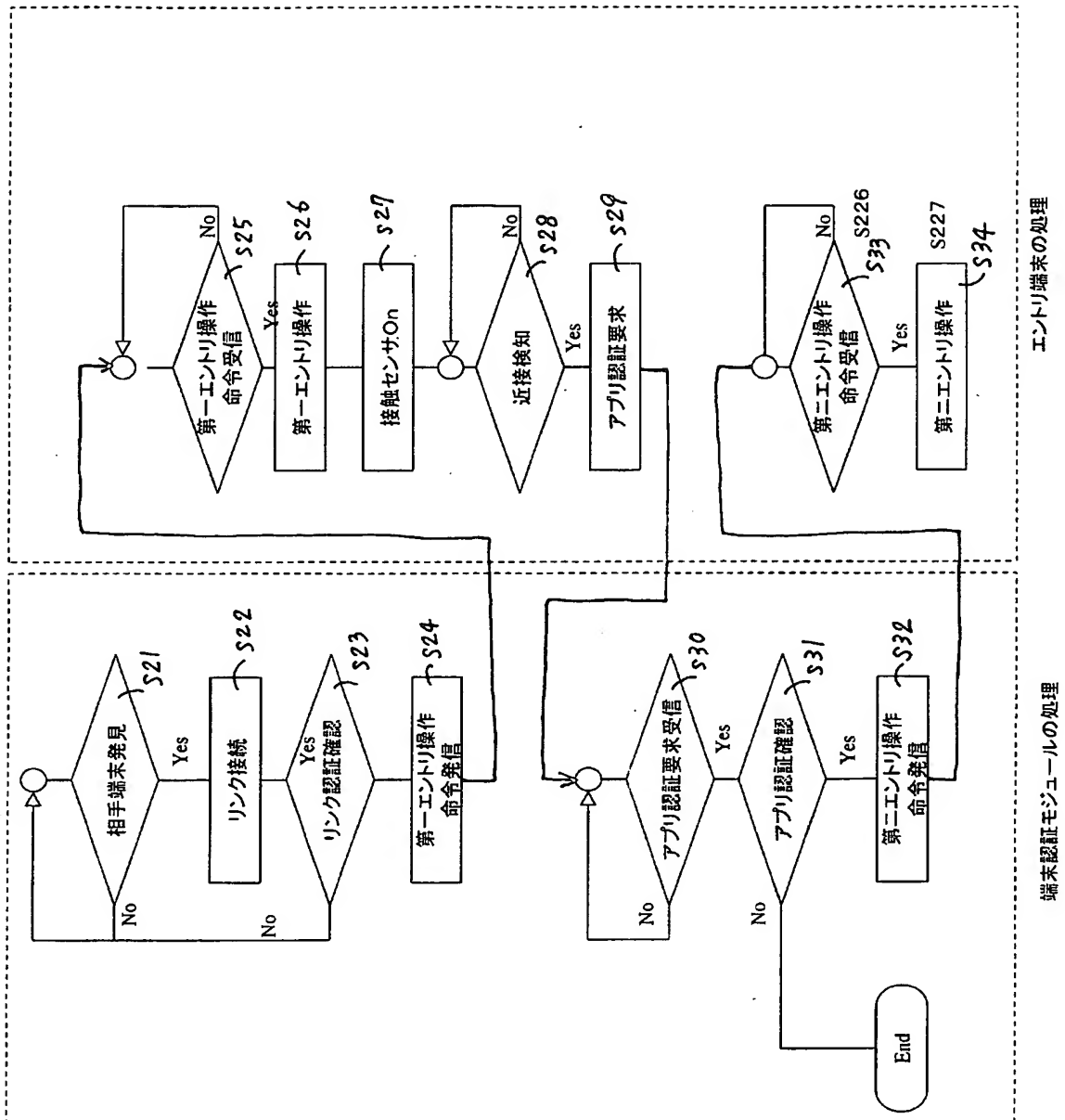




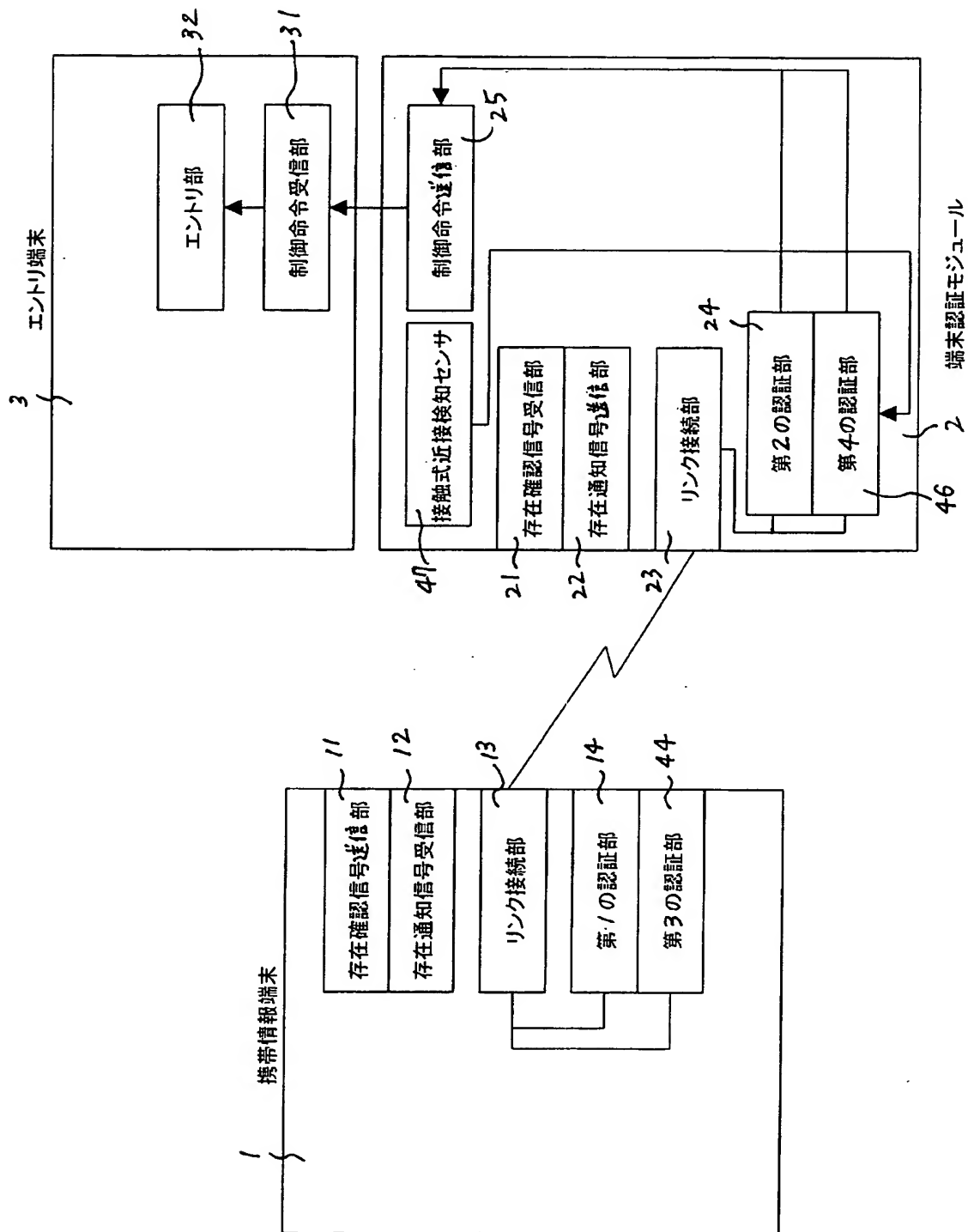
【図 9】



【図 10】



【図 11】





【書類名】 要約書

【要約】

【課題】 消費電力を削減でき、かつセキュリティ性を高くする。

【解決手段】 本発明に係る認証処理システムは、携帯情報端末 1 と、携帯情報端末 1 との間で無線にて認証処理を行う端末認証モジュール 2 と、端末認証モジュール 2 が携帯情報端末 1 との認証に成功した場合に車両のエントリ操作を行うエントリ端末 3 とを備えている。携帯情報端末 1 が第 1 の時間間隔ごとに存在確認信号を送信し、端末認証モジュール 2 が第 2 の時間間隔ごとに第 3 の時間間隔の間だけ存在確認信号を受信する受信モードに設定されるため、携帯情報端末 1 と端末認証モジュール 2 の双方とも消費電力を削減できる。

【選択図】 図 1



特願 2003-024501

出願人履歴情報

識別番号

[000003078]

1. 変更年月日      2001年   7月   2日  
[変更理由]      住所変更  
                    住 所      東京都港区芝浦一丁目1番1号  
                    氏 名      株式会社東芝
  
2. 変更年月日      2003年   5月   9日  
[変更理由]      名称変更  
                    住所変更  
                    住 所      東京都港区芝浦一丁目1番1号  
                    氏 名      株式会社東芝